

VirusFilter

Author: André Felipe Machado<clubes@techforce.com.br>

É um filtro antivírus tipo pipe through que interfaceia programas antivírus com leitores de email.

A avalanche de vírus está saturando as caixas postais. Embora não danifiquem as máquinas linux, consome muito tempo apagá-los manualmente.

Embora os programas antispam possam ser treinados para capturar estas mensagens de vírus, seria uma distorção de propósito.

Assim, ~~é anti-vírus específico para o filtro ClamAV~~ é anti-vírus específico para o filtro ClamAV mover para uma pasta específica.

VirusFilter é um script perl que interfaceia o ClamAV até com programas desktop, marcando as mensagens com um novo cabeçalho específico e que então pode ser usado para filtragem e classificação para alguma pasta, por exemplo.

Além do ClamAV rodando, você precisará de outros módulos perl que precisam ser baixados e instalados ANTES e em determinada ordem. Leia atentamente as instruções no próprio script.

O script não é de instalação óbvia. O público alvo são administradores de sistemas e usuários Unix e Linux com alguma experiência.

Se você usa Debian GNU Linux, a tarefa pode ser mais fácil.

Configurei meu Kmail para fazer um pipe de todas mensagens pelo virusfilter.pl como a primeira regra de filtragem. Você pode fazer diferente e também pode fazer este pipe no servidor, se preferir.

O script lê da STDIN e escreve na STDOUT. Traduzindo: seu programa de email (ou script)

deverá fazer um pipe da mensagem e a recolher de volta na saída. No Kmail isto é fácil (já instruído nesta página, para os programas antispam). Outros programas também possibilitam isso.

Você precisará manter a base de dados de vírus atualizada, pelo programa freshclam. Todos os dias. No site do ClamAV, você poderá submeter amostras de novos vírus que não tenham sido capturados. Também encontra um how-to de como gerar você mesmo assinaturas para novos vírus sem ter de esperar a atualização da base de dados oficial! Em redes de alto tráfego, algumas horas expostas a um novo vírus pode ser tempo demais. É MUITO vantajoso ter esse poder de criar assinaturas de vírus.